Hackmaggeddon
Witness of Cyber War

Paolo Passeri
System Engineer
Lastline, Inc.

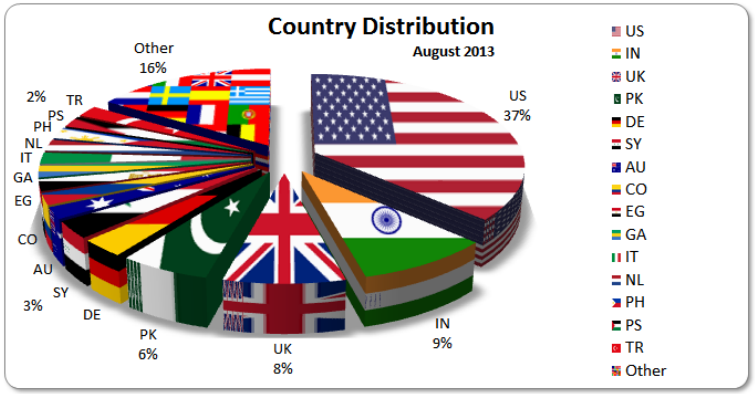
Agenda

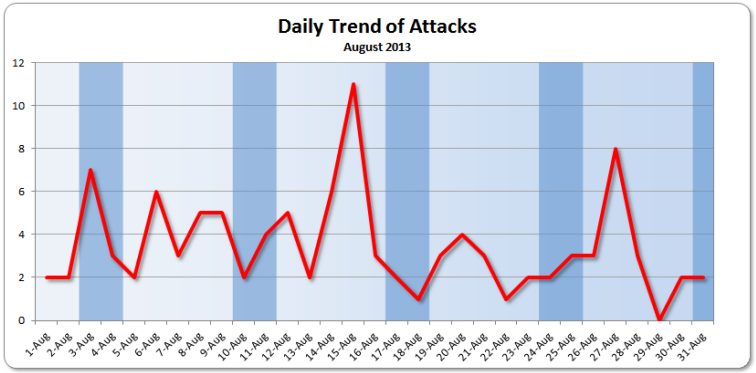
- Introduction
- 3 Years Of Breaches
- Attack Trend
- Motivations
- Techniques
- Focus On Targeted Attacks
- Several Examples of Cyber Wars

What is Hackmageddon?

- Since March 2011 Hackmaggeddon.com collects timelines related to the main Cyber Attacks in a bi-weekly basis.
- Only sources freely available on the Internet are taken into consideration (specialized news sites, hacking blogs, etc.).
- Born to collect useful data for the curator's pre sale activity, it has grown beyond the initial expectations, offering a useful synoptic picture of what's going on the cyber space.
- 30,000 visits per month

Hackmageddon Stats





Since March 2011 to date, Hackmageddon.com has collected data related to:

- 418 attacks (Jul-Dec 2011)
- 1320 attacks (2012)
- 1027 attacks (Jan-Sep 2013)

They can be useful to derive stats for analyzing how trends vary during the years and are influenced by global events.

Caveats

- The sample is heterogeneous and stats cannot obviously be exhaustive! They are useful to understand the trends but cannot include all the attacks (have a look to Zone-H to see how many defacements happen each second);

- Sample of 2011 only involves 8 months;

- Defacements are taken into consideration only if targeting primary domains of high-profile sites (primary companies or Governments);

Caveats (2)

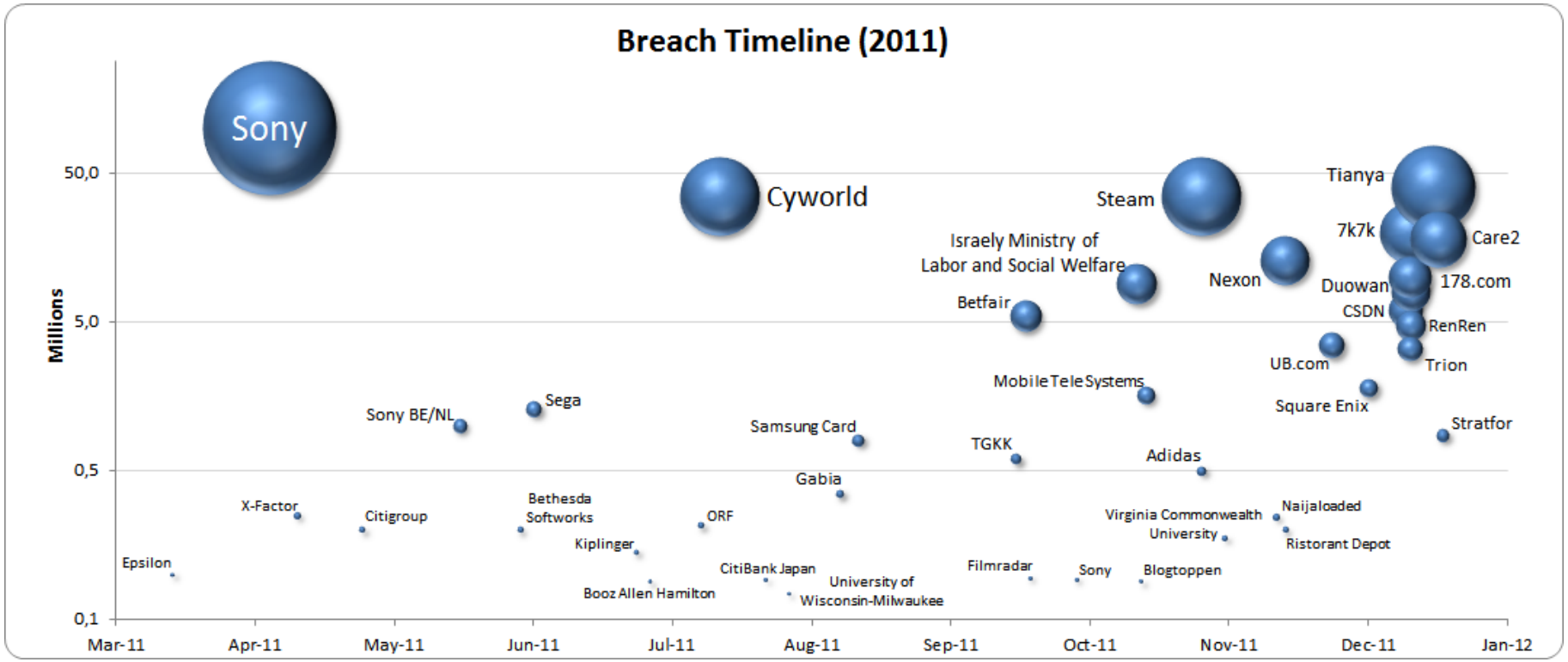
- Hacktivism-led attacks aim to attract the attention of media, so advertise themselves on forums and news sites. In many cases the reputation of the sources is controversial.

- On the other hand, targeted attacks are stealth and (too) often discovered only after they have achieved their scope.

Agenda

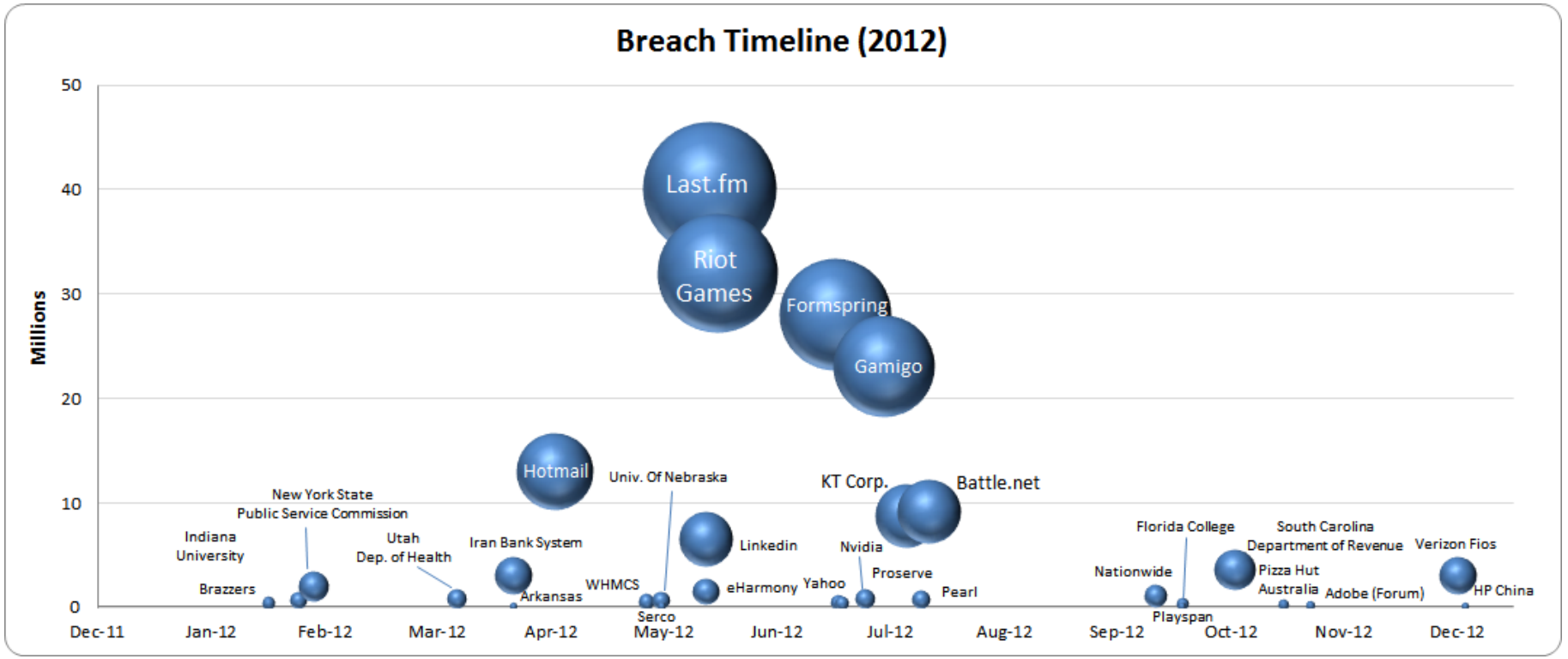
- Introduction
- 3 Years Of Breaches
- Attack Trend
- Motivations
- Techniques
- Focus On Targeted Attacks
- Several Examples of Cyber Wars

Size Matters (2011)
Main Breaches with ≥ 100.000 records



The total is around **322M** leaked accounts

Size Matters (2012)



The total is around **180M** records

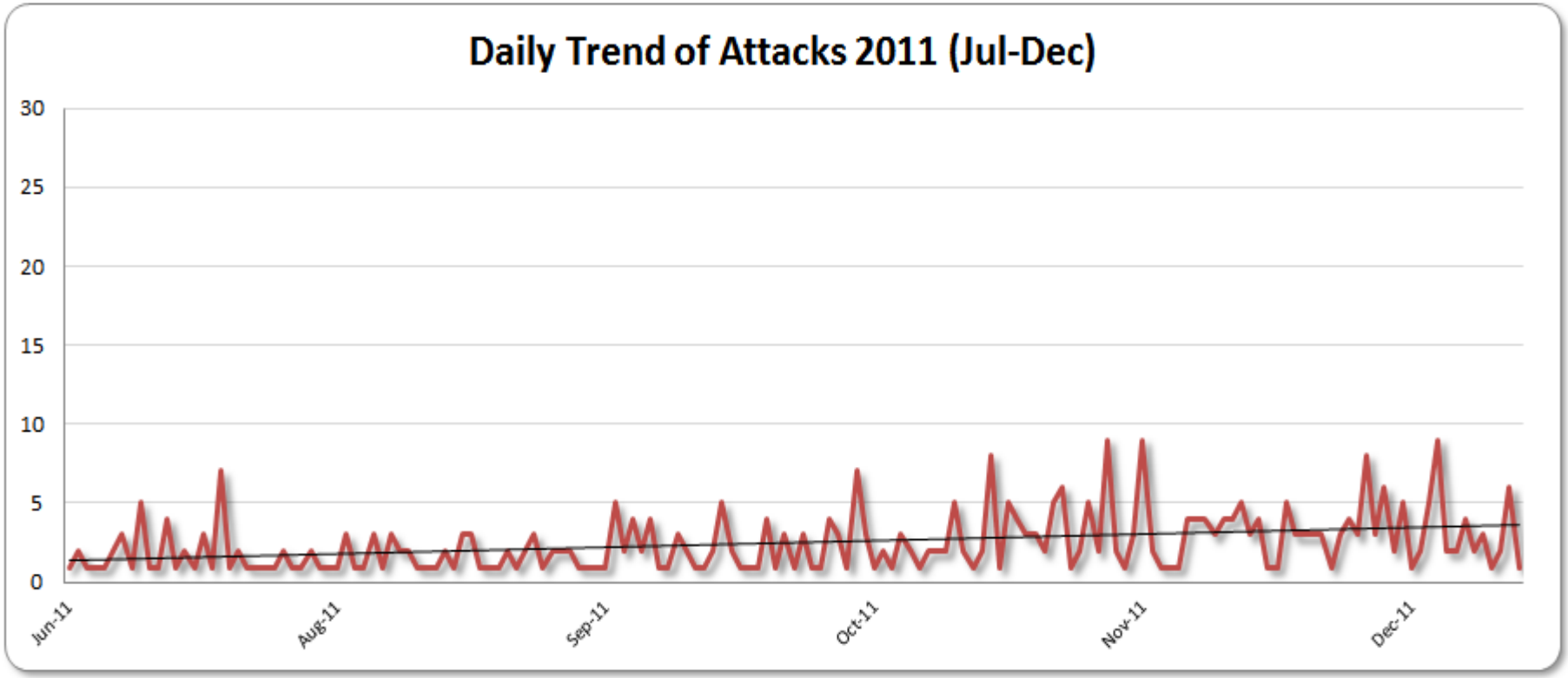
Size Matters (2013)

Total (up-to-date) is around **199M** records

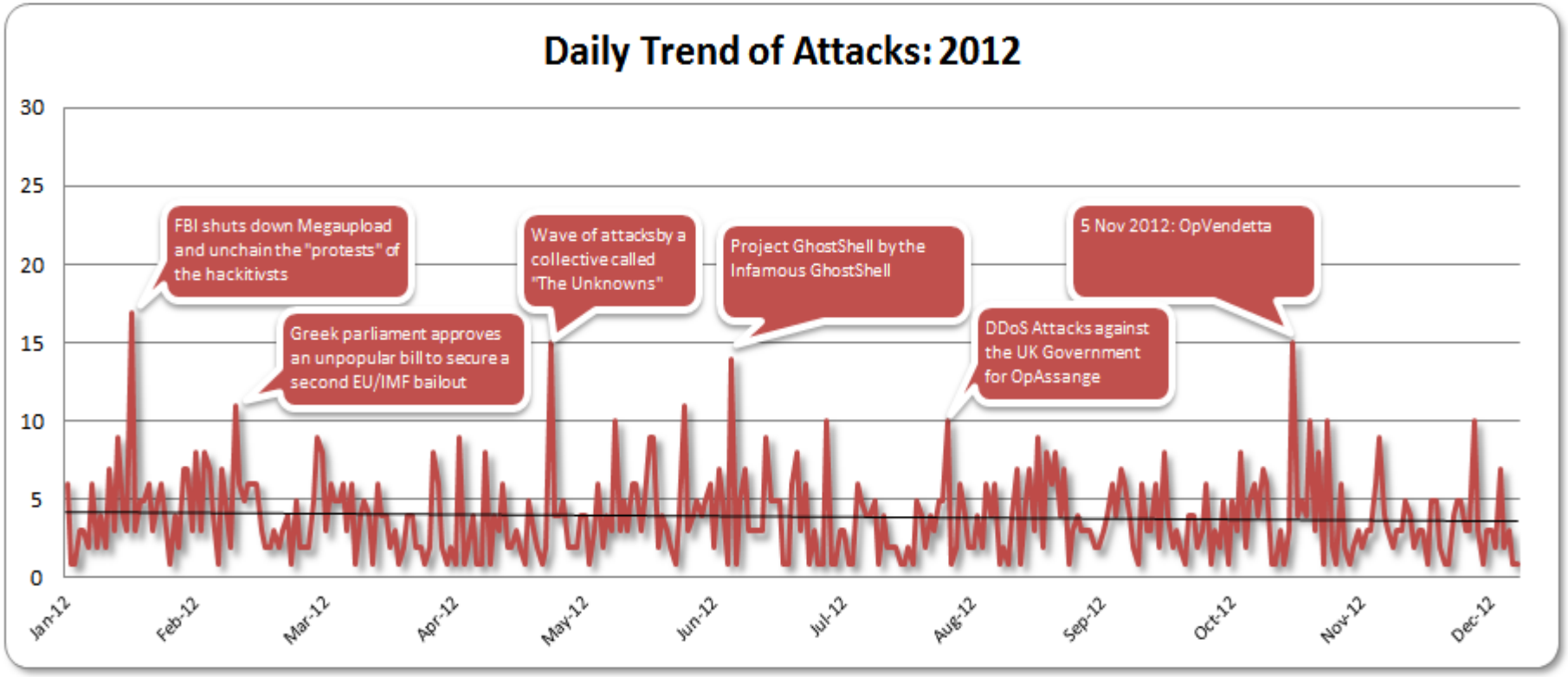
Findings

- Introduction
- 3 Years Of Breaches
- Attack Trend
- Motivations
- Techniques
- Focus On Targeted Attacks
- Several Examples of Cyber Wars

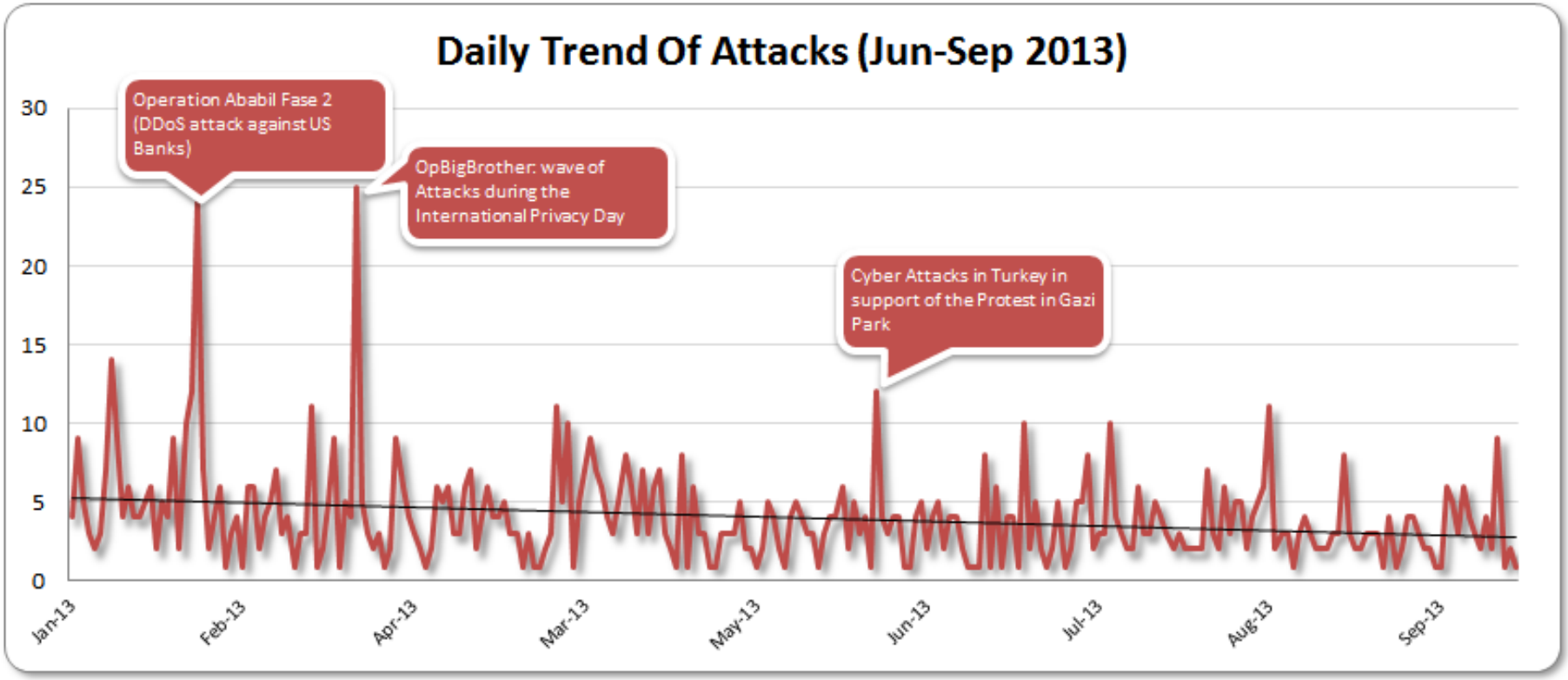
Attack Trend: 2011 (8 Months)



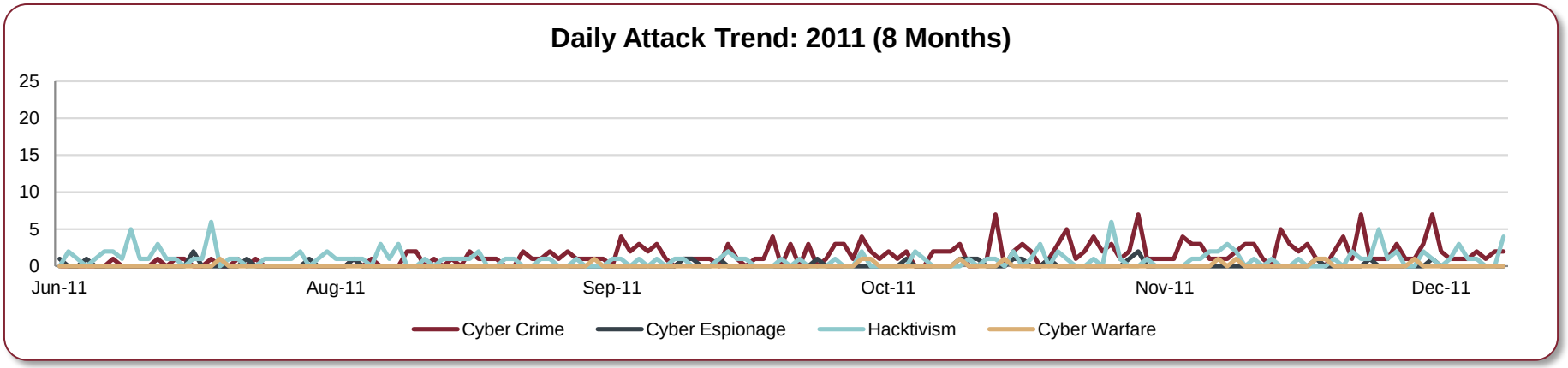
Attack Trend: 2012

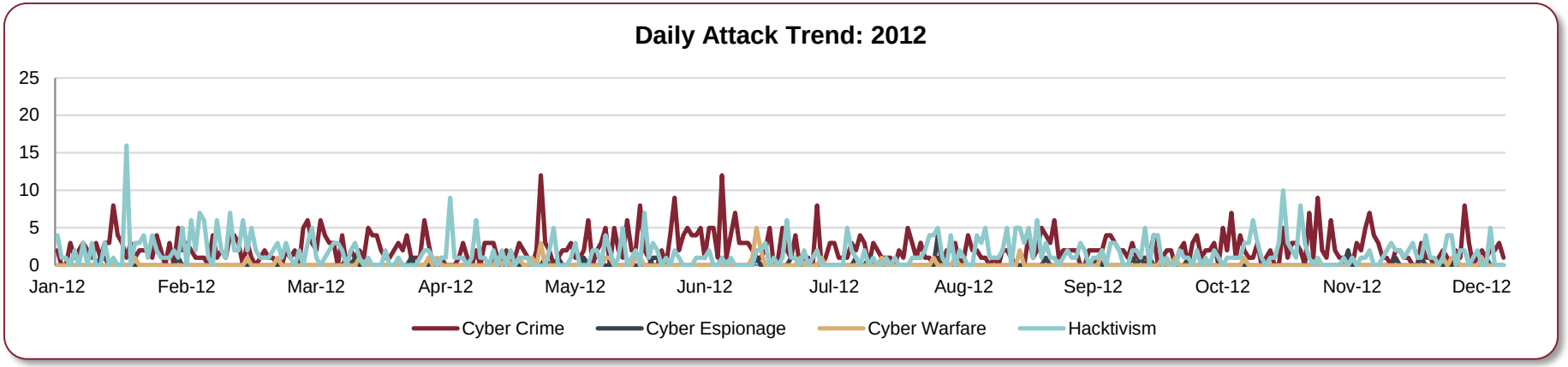


Attack Trend: 2013 (9 Months)

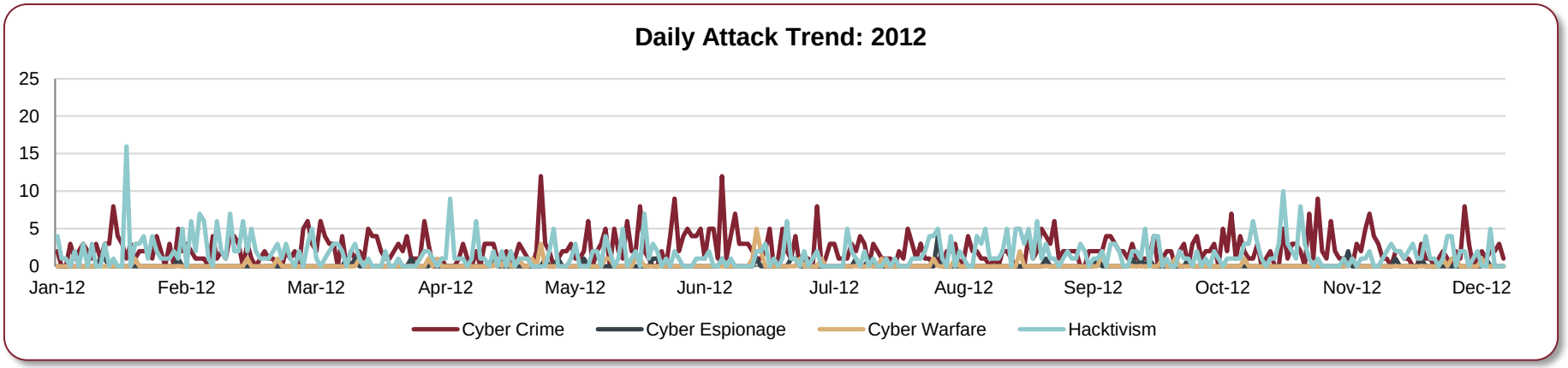


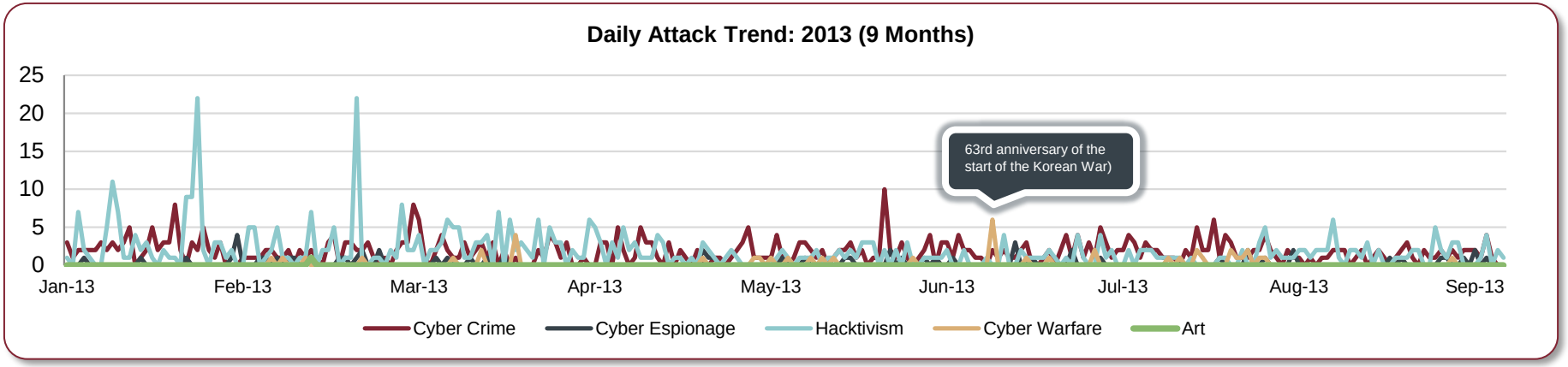
Daily Attack Trend: 2011 to 2012





Daily Attack Trend: 2012 to 2013





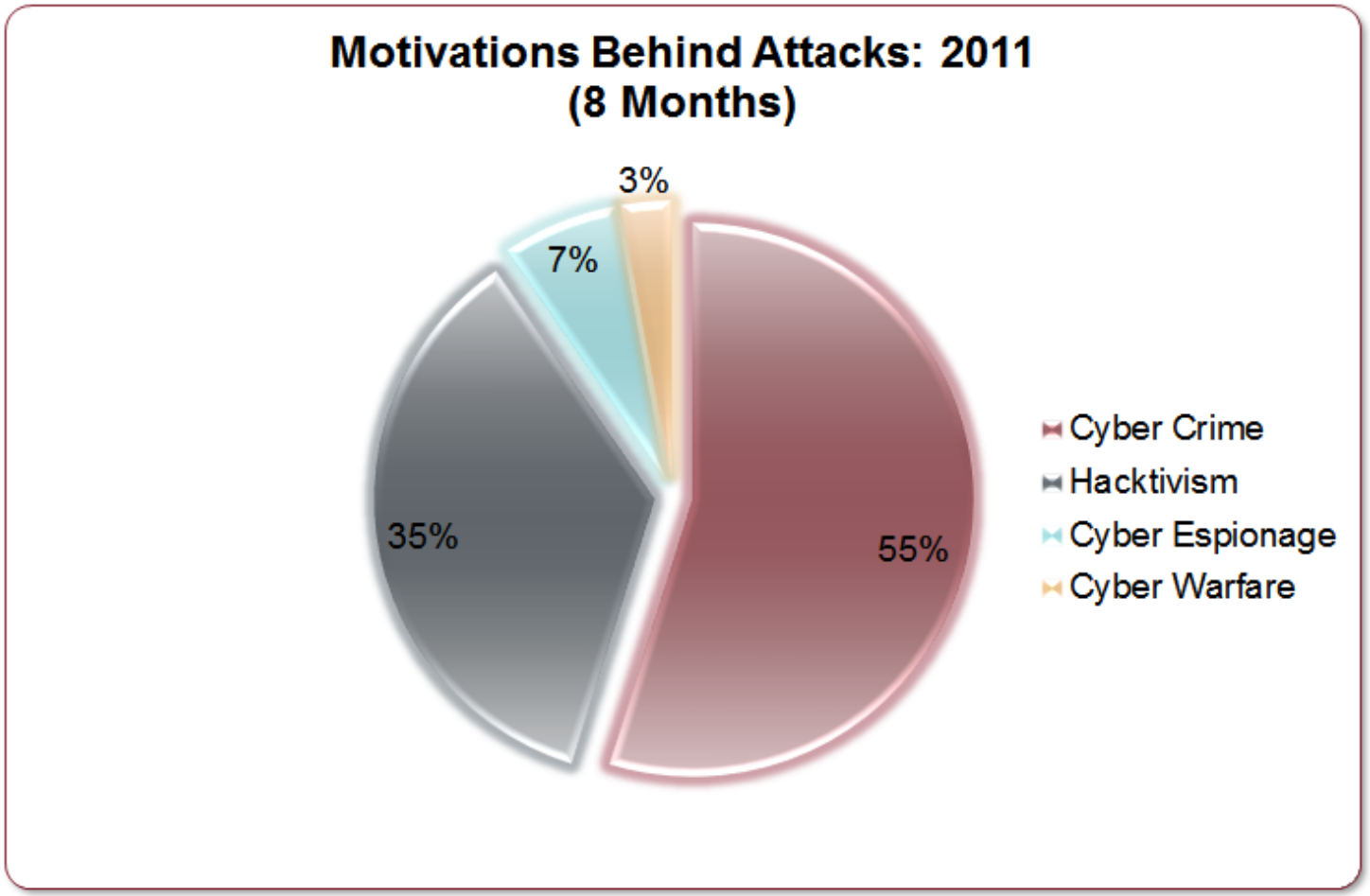
Findings

- Over the “background noise” the peaks are often due to hacktivism-driven attacks;
- They aim to attract the attention of media and in most cases are executed as a reaction to external events (Greece, Egypt and Turkey);
- In the second part of 2013 they have been “diluted” rather then being concentrated in peaks
- Several Operations have been a fiasco (OpPetrol, OpIsrael)
- Obviously, targeted attacks do not look for media coverage and are often discovered after their execution.

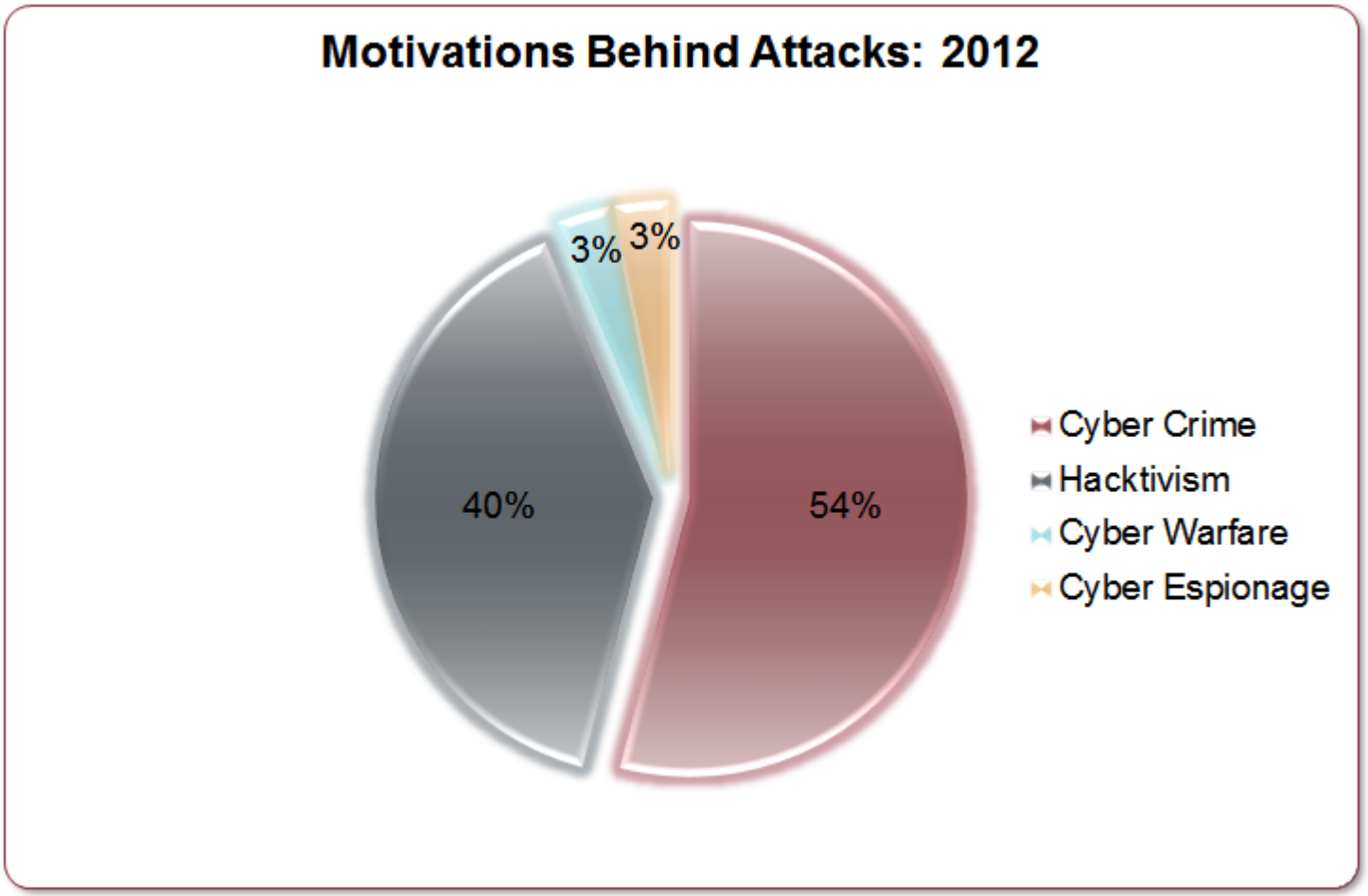
Agenda

- Introduction
- 3 Years Of Breaches
- Attack Trend
- Motivations
- Techniques
- Focus On Targeted Attacks
- Several Examples of Cyber Wars

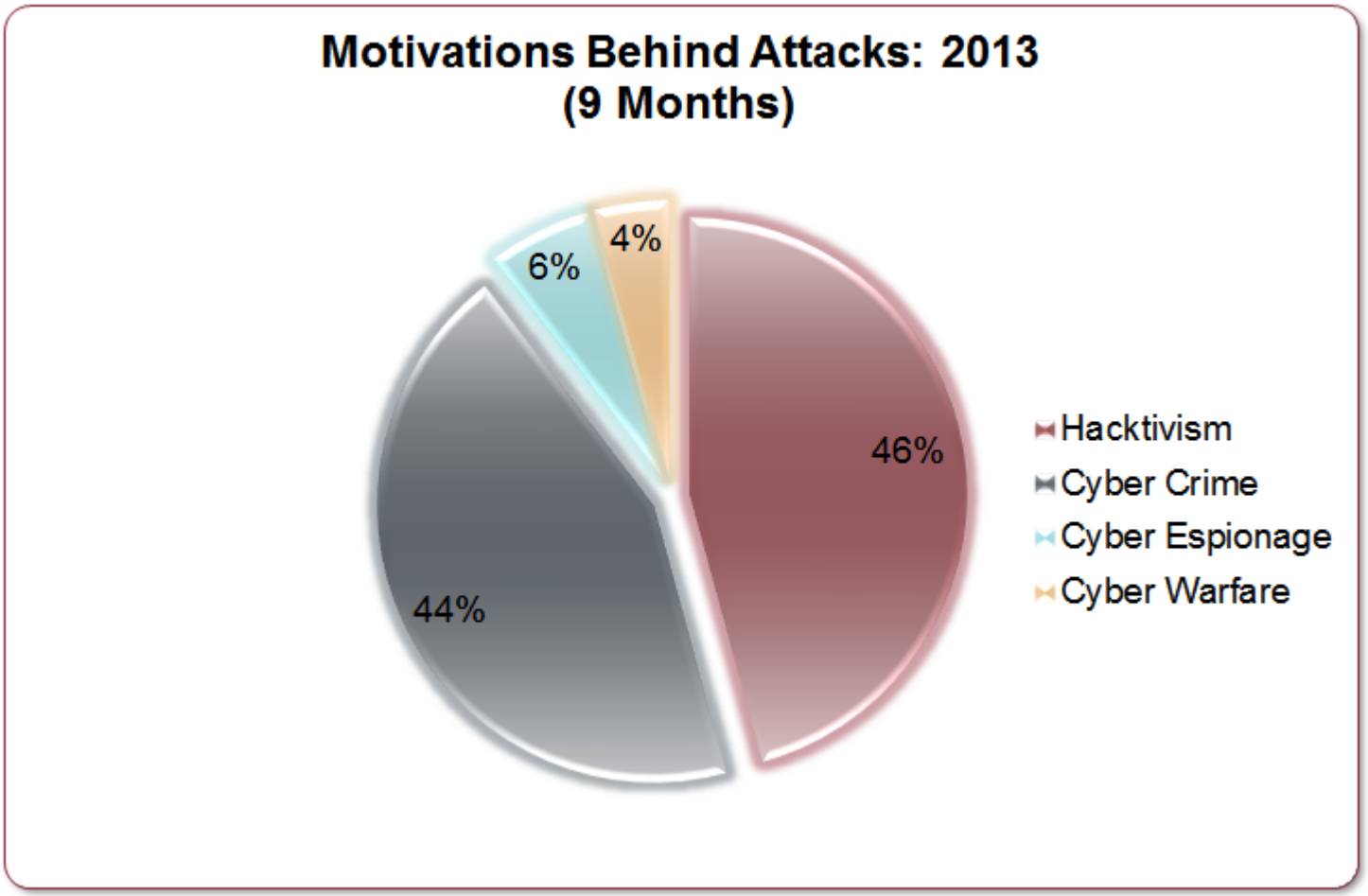
Motivations Behind Attacks: 2011 (8 Months)



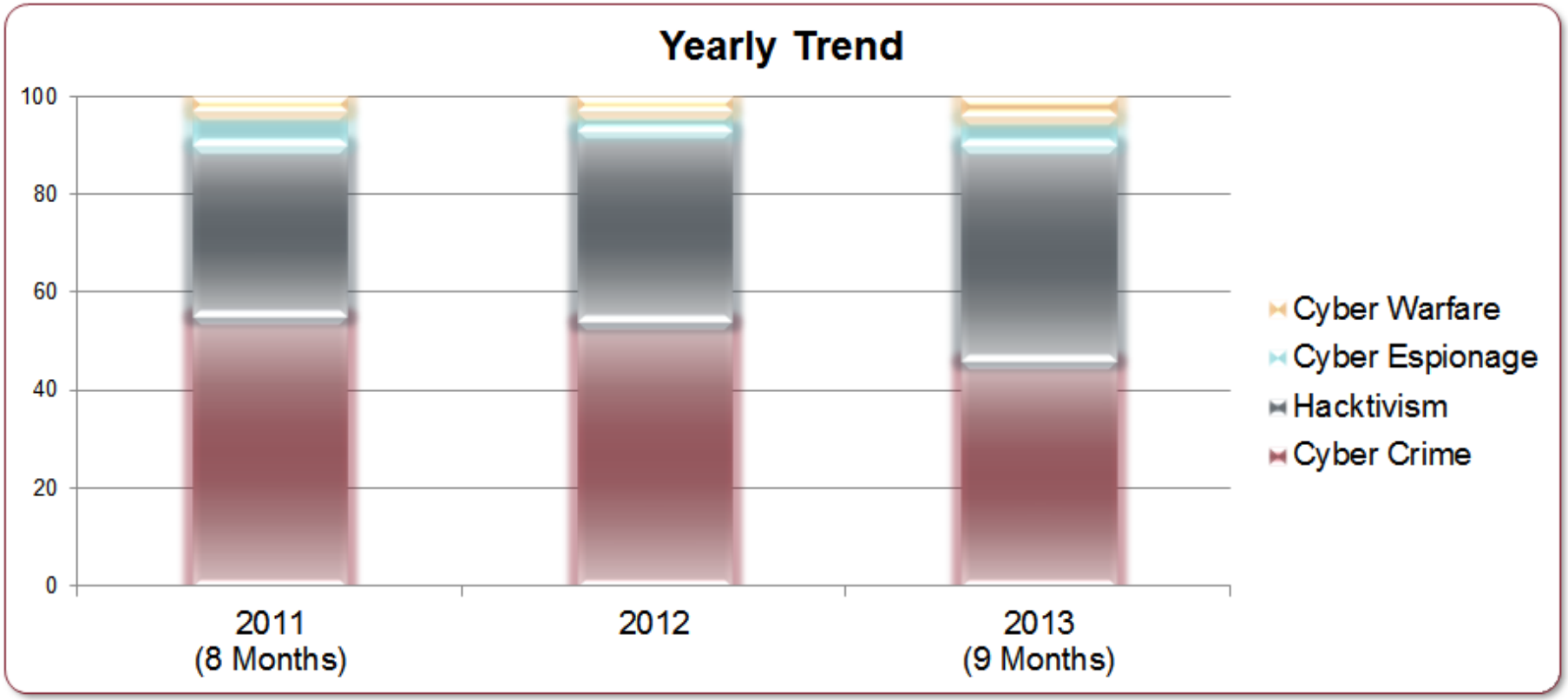
Motivations Behind Attacks: 2012



Motivations Behind Attacks: 2013 (9 Months)



Motivations Behind Attacks: Yearly Trend



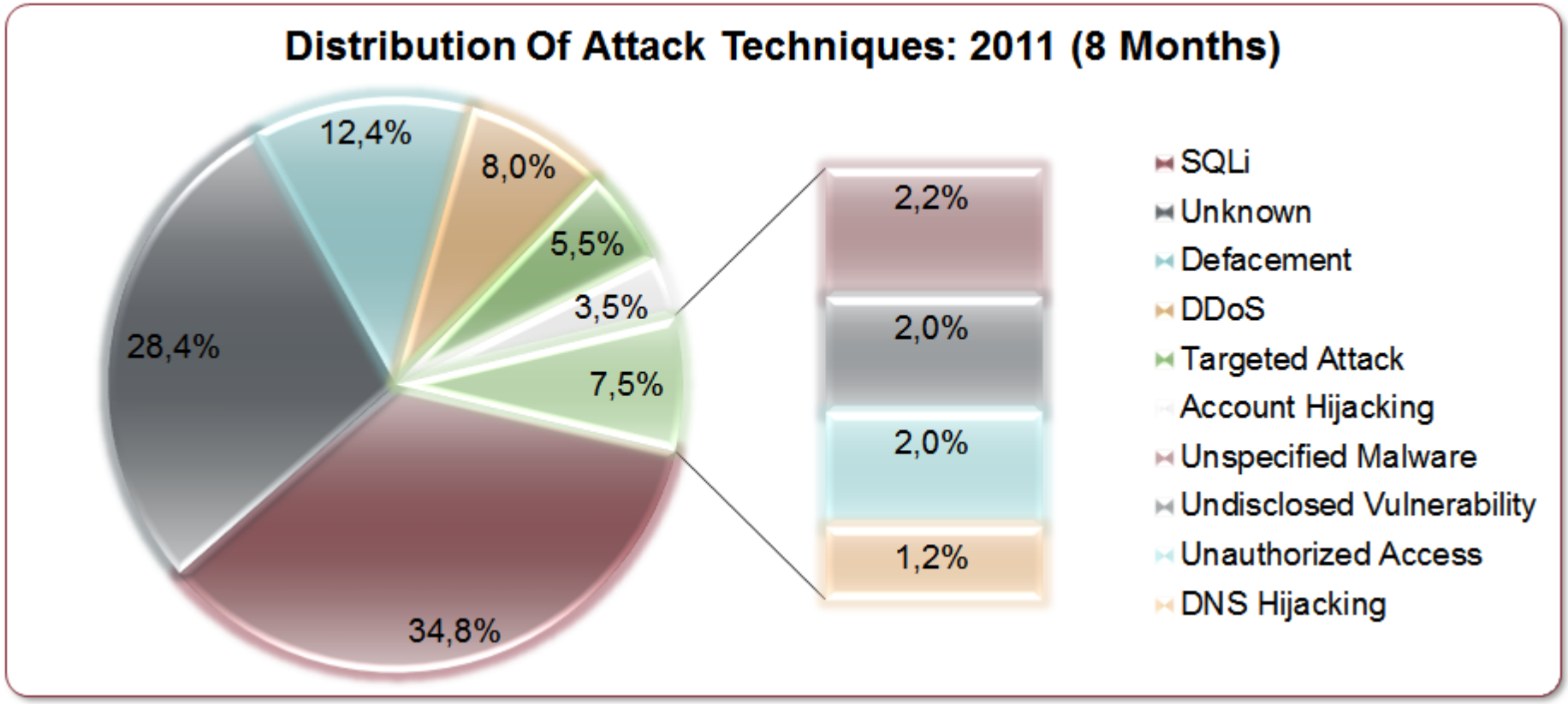
Findings

- Despite the actions performed by the Law Enforcement Agencies, 2013 is showing an increase of attacks related to hacktivism;
- This is partly due to the political turmoil (in Greece, Turkey, Egypt and Syria), but also to new unprecedented forms of Hacktivism such as the DDoS attacks to the U.S. Banks.
- Particularly meaningful is the evidence that sophisticated cyber attacks operations are steadily gaining space on the media (6% of attacks recorded in 2013, so far, are related to Cyber Espionage Operations).
- Maybe in 2012 Hacktivists gained more attention and shadowed State sponsored Operations?

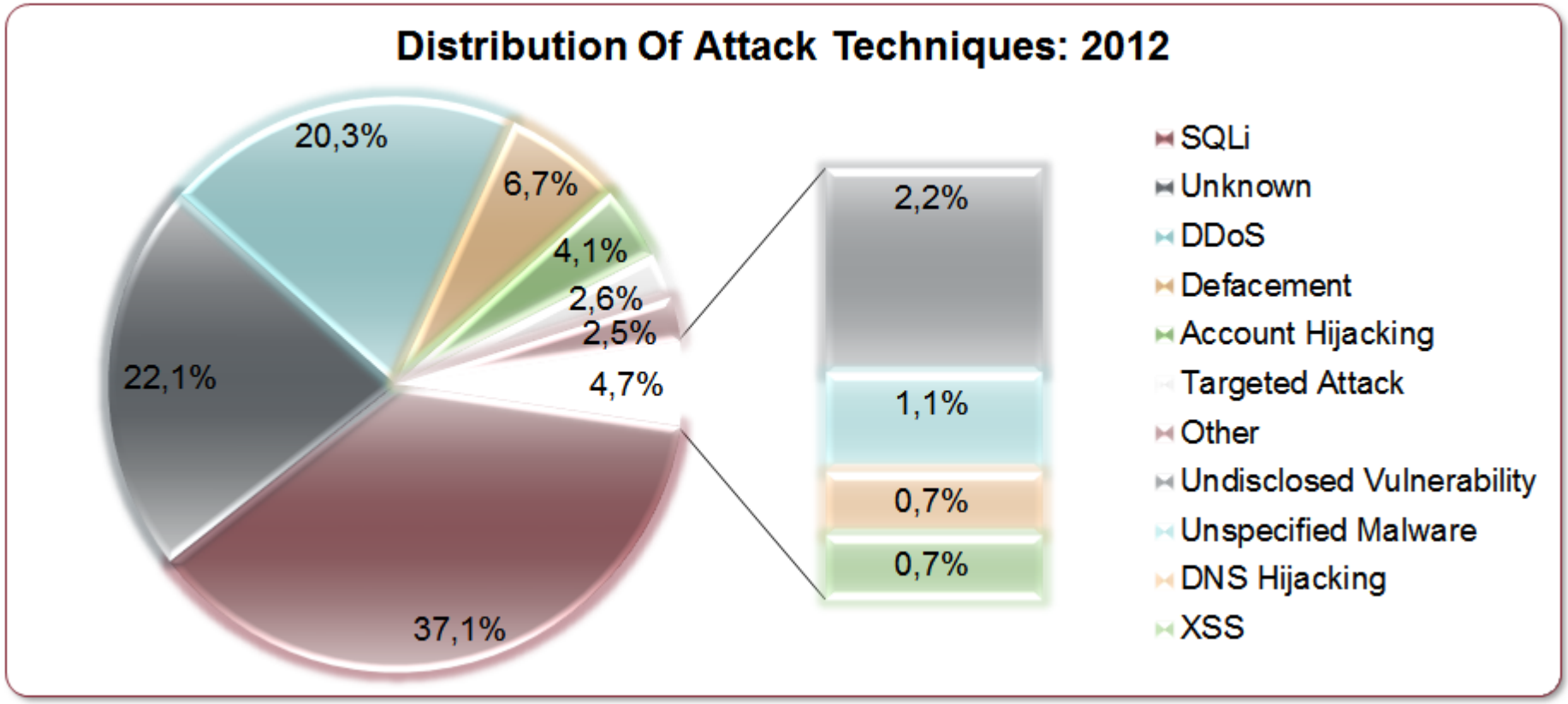
Agenda

- Introduction
- 3 Years Of Breaches
- Attack Trend
- Motivations
- Techniques
- Focus On Targeted Attacks
- Several Examples of Cyber Wars

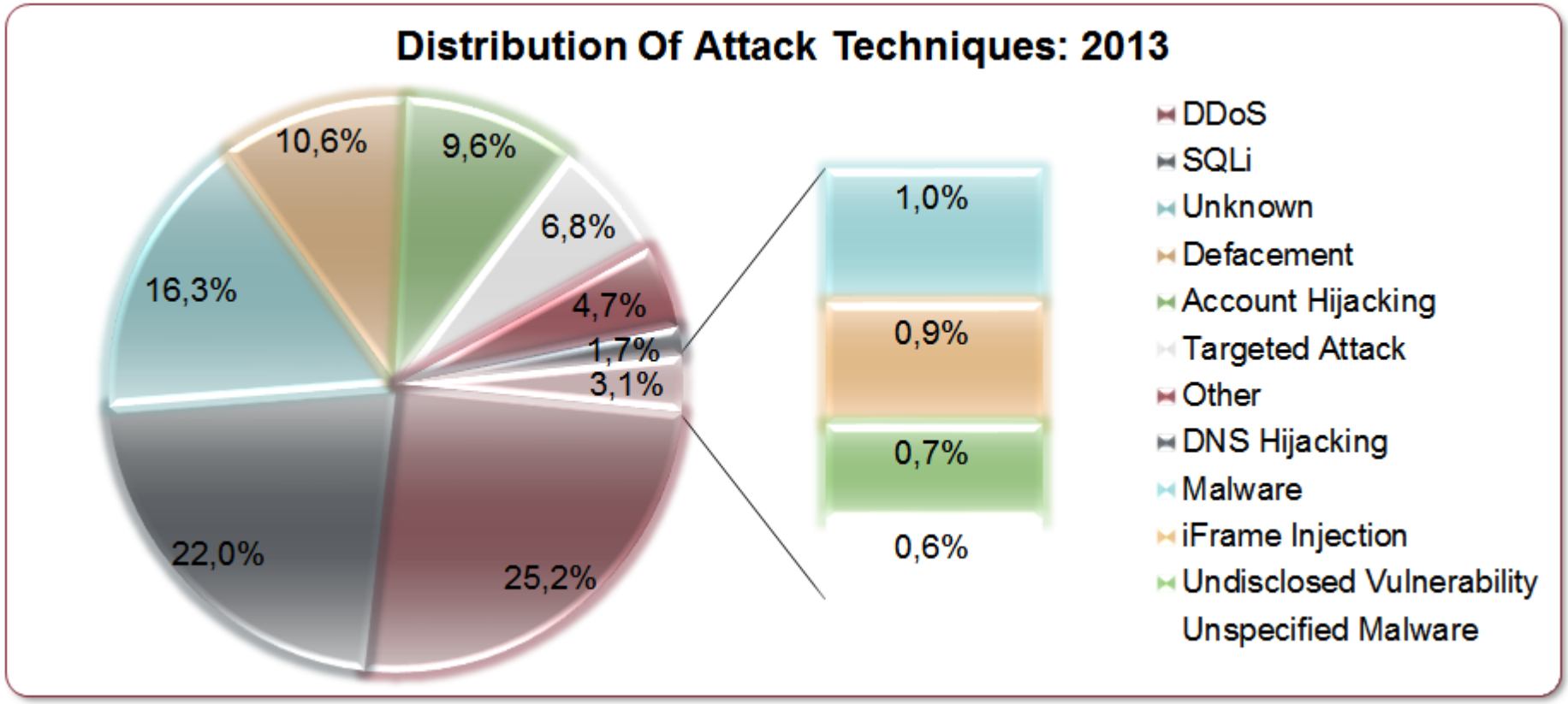
Distribution of Attack Techniques: 2011 (8 Months)



Distribution of Attack Techniques: 2012



Distribution of Attack Techniques: 2013 (9 Months)



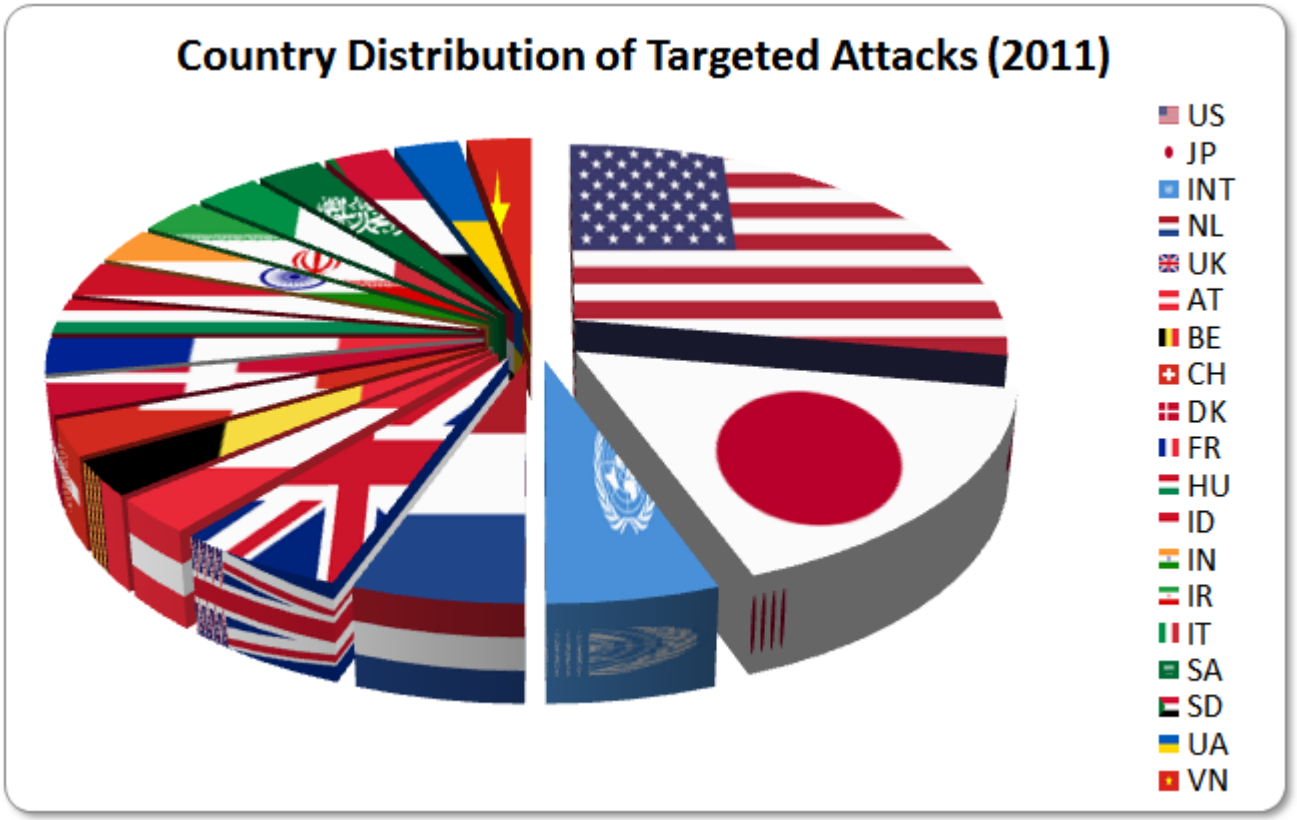
Findings

- DDoS is the favorite weapon of hacktivists. Attacks using this technique gained more space in the news in 2013 (think to the wave of attacks against US Banks).
- Account Hijackings had nearly a 100% increase on a yearly basis (on the wake of the actions of the Infamous Syrian Electronic Army): Maximum result with minimum effort.
- Targeted attacks revealed in the news jumped (so far) from 2.5% to 6.8%.
- Apparently high profile targets have become more aware of SQLi risks.
- In too many cases the reason of the attacks is still unknown.

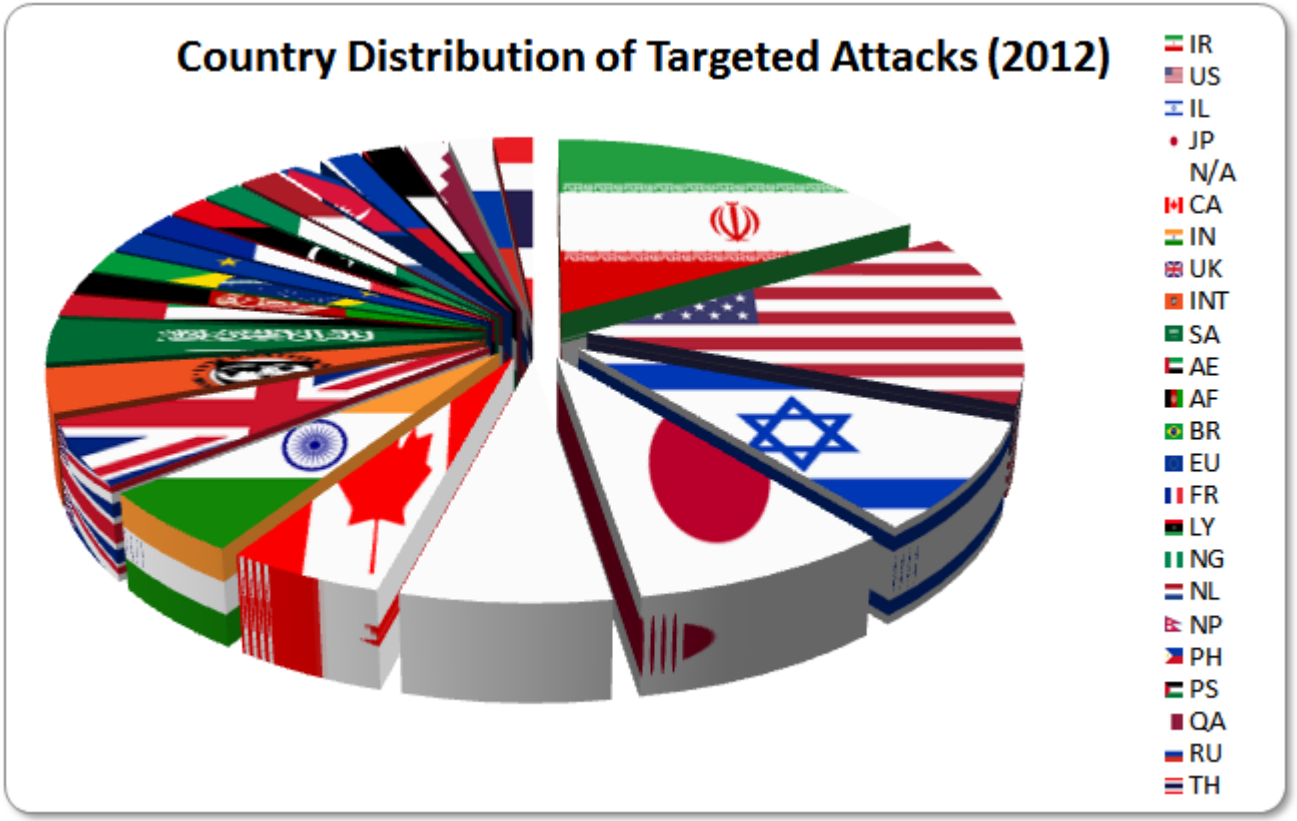
Agenda

- Introduction
- 2 Years Of Breaches
- Attack Trend
- Motivations
- Techniques
- Focus On Targeted Attacks
- Several Examples of Cyber Wars

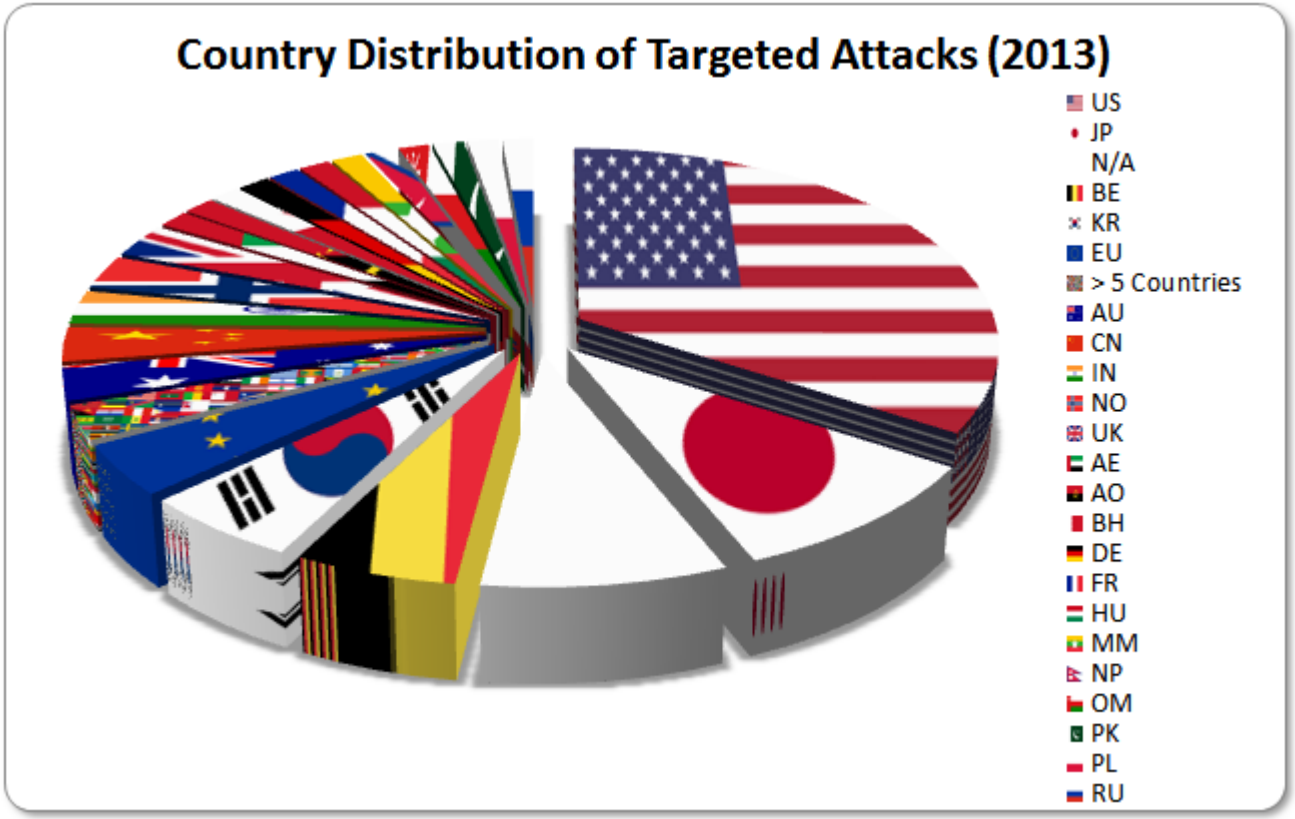
Focus on Targeted Attacks: 2011 (8 Months)



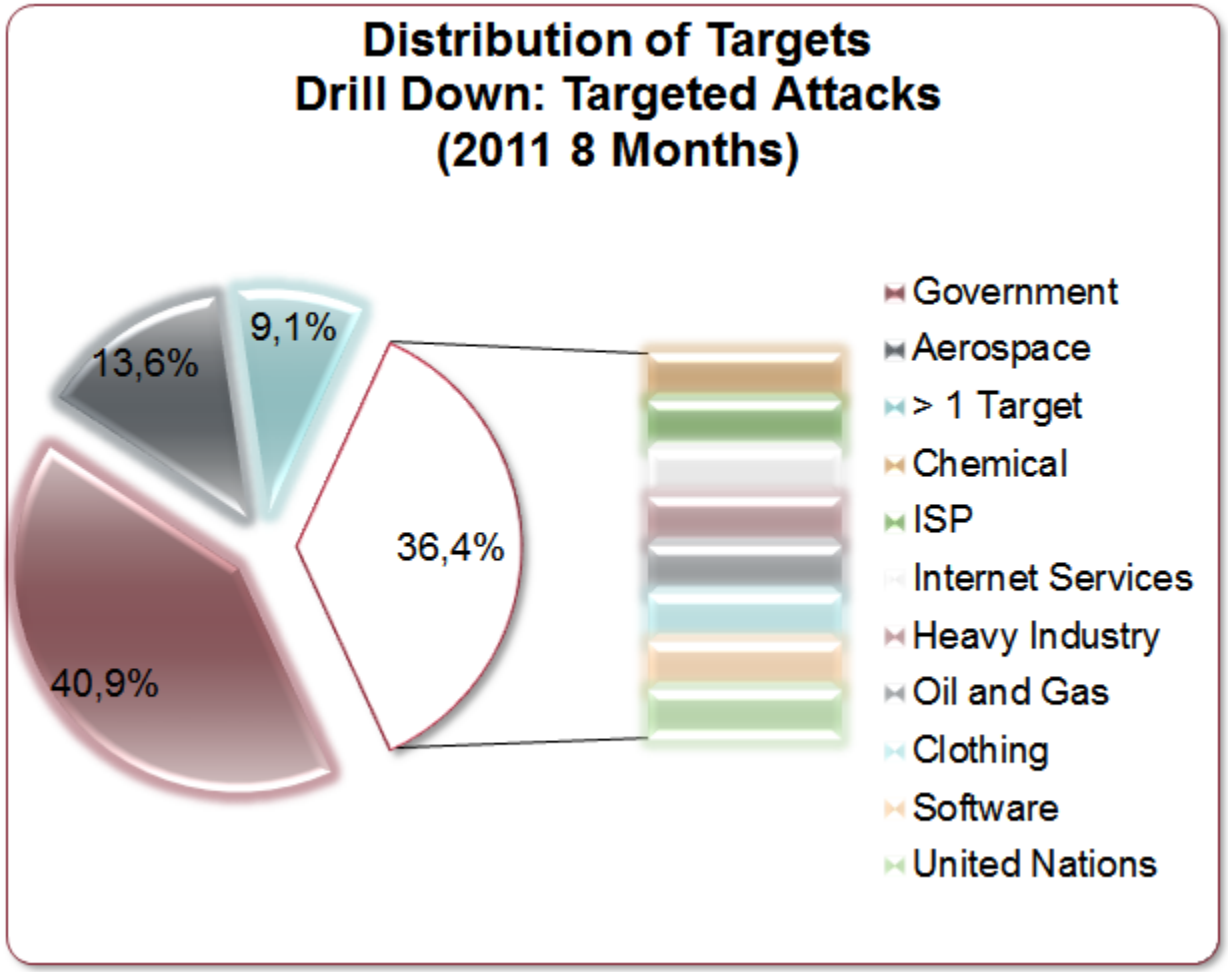
Focus on Targeted Attacks: 2012



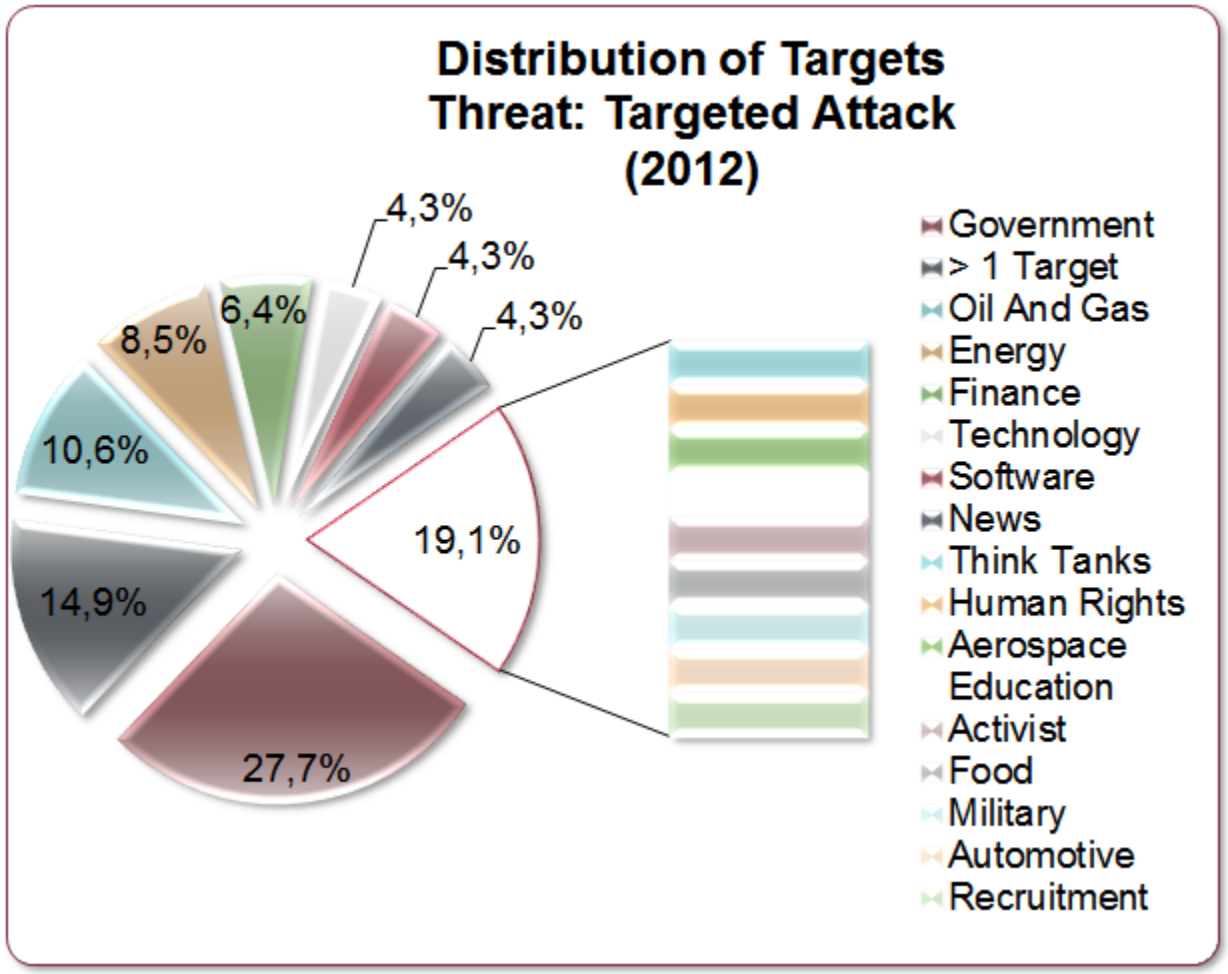
Focus on Targeted Attacks: 2013



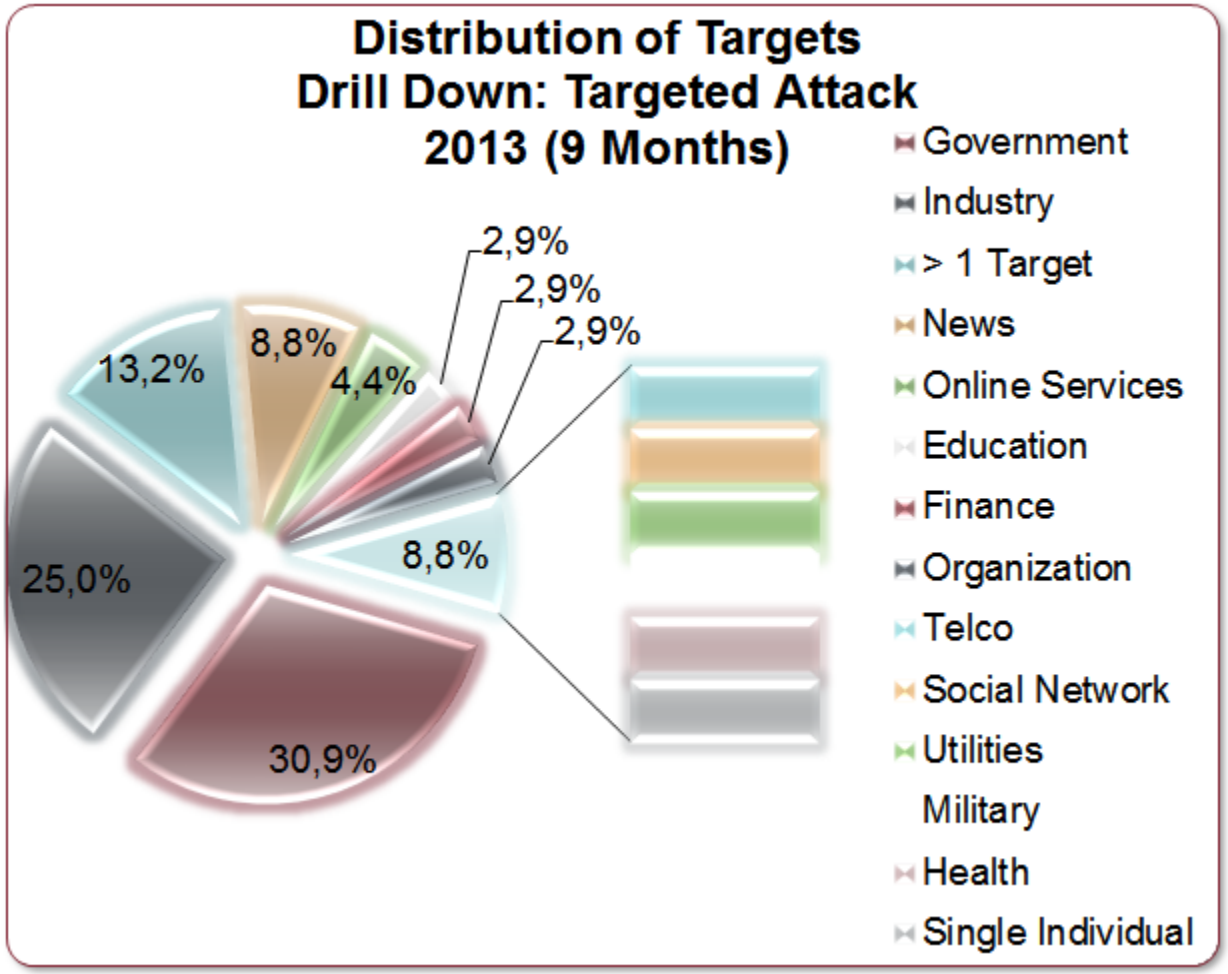
Drill Down 2011



Drill Down 2012



Drill Down 2013



Findings

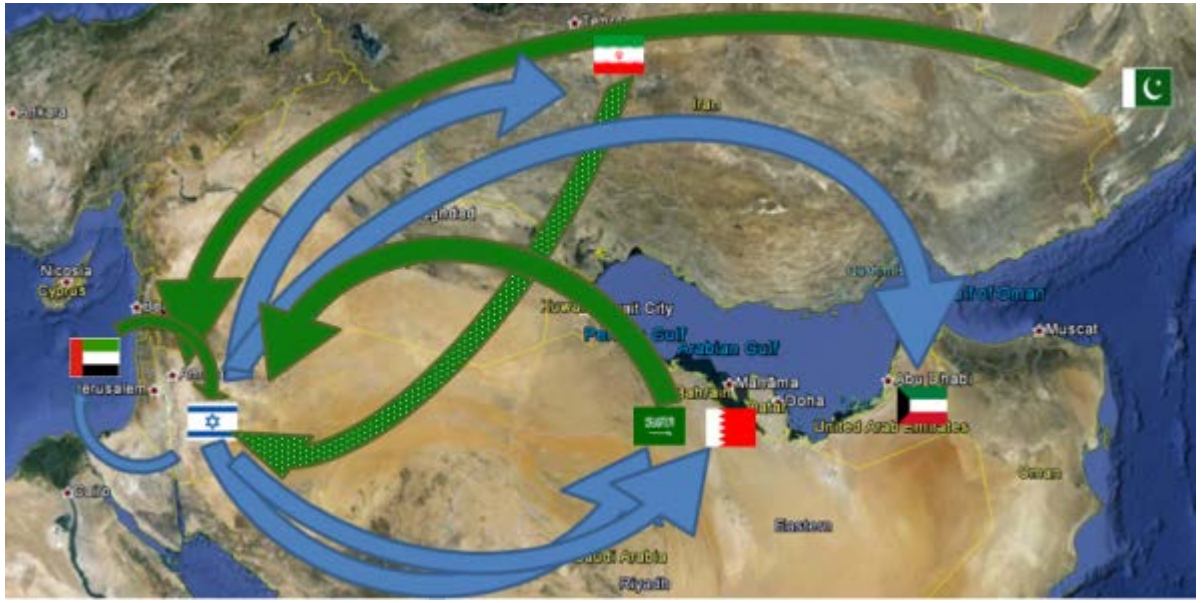
- Apparently 2012 has been a hard year for Iran. Unfortunately in many cases (except for Flame) no many details have been disclosed.
- 2013 has brought a new awareness for the US (APT-1, attacks to Apple, Facebook and Microsoft)
- Even Japan has a regular presence in the podium!
- Governments are the top targets!

Agenda

- Introduction
- 2 Years Of Breaches
- Attack Trend
- Motivations
- Techniques
- Focus On Targeted Attacks
- Several Examples of Cyber Wars

Focus On: Middle East Cyber War

Between January and March 2012, the Middle East has seen an unprecedented event: a real Cyber War fought between Pro-Arab and Pro-Israeli Hackers.



Unlike Conventional Wars, singe individual are not collateral victims, but in many cases are the real targets.

A model precursor of the next century Wars?

	Pro-Arab Hackers	Pro-Israeli Hackers
Credit Cards Leaked	448.000,00	11.000,00
Accounts Leaked	170.000,00	5300
Details of Single Individuals Leaked	300.000,00	140.000,00
Emails Leaked	15.000,00	105.000,00

More on: http://hackmageddon.com/middle-east-cyber-war-timeline/

Other Noticeable Cases

- **China Vs Philippines:** Brilliant Example of an asymmetric cyberwar unchained by a real dispute concerning the sovereignty on the Scarborough Shoal and the Spratly Islands:

  More on: http://hackmageddon.com/2012/05/01/philippines-and-china-on-the-edge-of-a-new-cyber-conflict/

- **India Vs Pakistan Vs Bangladesh:** each one of the three countries is engaged in a cyber conflict with the other two.

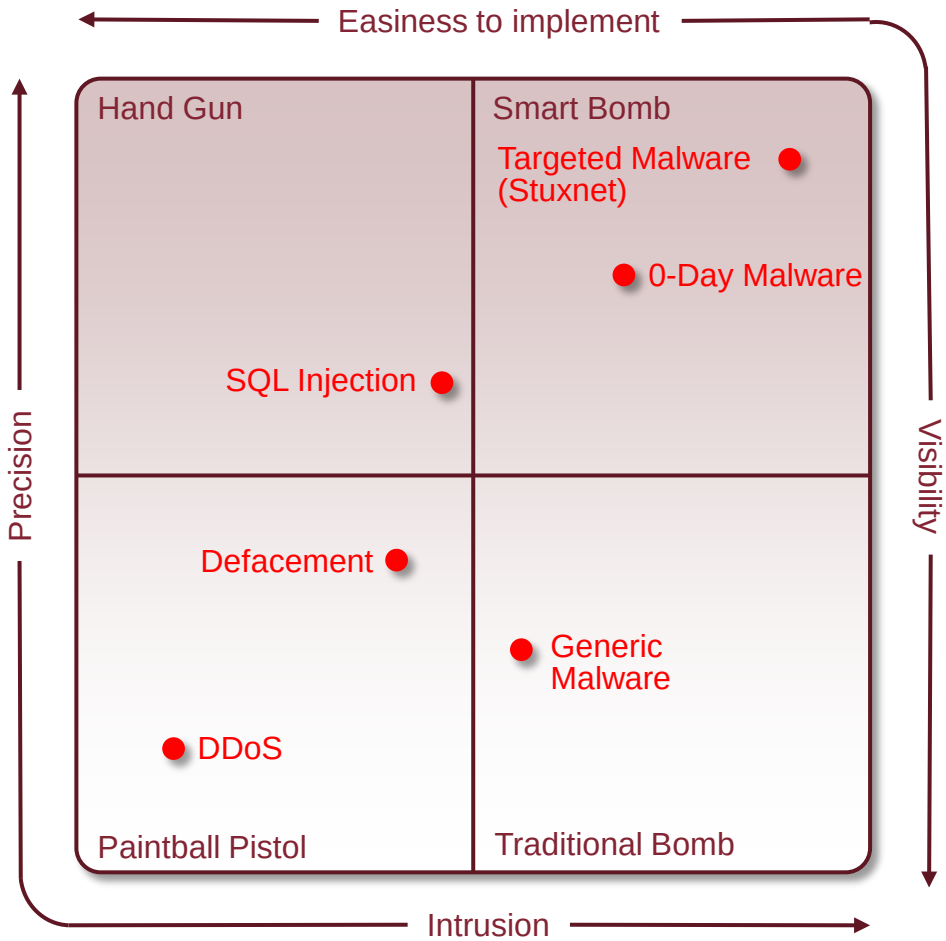
  More on: http://hackmageddon.com/2012/03/24/timeline-of-cyber-war-between-bangladesh-and-india/, http://hackmageddon.com/2013/08/22/timeline-of-cyber-attacks-in-conjunction-with-the-pakistan-and-india-independence-days/

- Despite the tensions in the real world, in both cases the cyber war is "limited" to Defacements (at least so far!): state sponsored operations are fought on a well different plan and often invisible.

Conclusions

- The number of attacks motivated by hacktivism reported in the news is constantly increasing. This is partly due to the political turmoil but also to new unprecedented forms of Hacktivism.
- A year-to-year comparison (2012-2013) shows that targeted attacks revealed in the news jumped (so far) from 2.5% to 6.8%. Governments are top targets of this category.
- Although cyber wars may be fought in multiple ways, the most damaging ones are stealth…

A (Possible) Classification of Cyber Weapons



hackmageddon.com

Questions?